



Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendments, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on February 6, 2006.


Peter Borghetti
Reg. No. 42,343

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/037,382	Confirmation No. 6806
Applicants	:	Joseph Claude Caci et al.	
Filed	:	January 4, 2002	
Priority date	:	January 4, 2002	
TC/A.U.	:	3677	
Examiner	:	Michael J. Kyle	
Title	:	PURCHASING AID LOGISTICS APPLIANCE	
Docket No.	:	12078-129	
Customer No.	:	26486	

Burns and Levinson, LLP
One Beacon Street 30th Floor
Boston, MA 02108-2106
(617) 854-4000

TO: Mail Stop Amendments
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

DECLARATION UNDER 37 CFR 1.132

I, Thomas J. Leso, declare that:

(1) I am a person of ordinary skill in the art of Computer Science as evidenced by my background in the field of Computer Science and Engineering and Information Sciences and Technology:

(a) Education: BS, Computer Science, BS, Mathematics, MS, Computer Science, Ph.D., Instructional Systems Design, Penn State University (1970, 1970, 1971, 1994)

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

(b) Current position (1980 – present): Instructor of Computer Science and Engineering, Penn State Altoona, Altoona, PA; and (2005-present) Adjunct Instructor of Information Sciences and Technology, Continuing Education, Penn State University, University Park, PA;

(c) Previous positions, many of which have involved systems and software engineering and standards for government and business contracts, including security standards and mechanisms:

(i) 1978-1980: Principal Engineer, HRB Singer, Inc., State College, PA;

(ii) 1975-1978: The Mitre Corporation, McLean, VA;

(iii) 1972-1975: TRW, Inc., McLean, VA; and

(iv) 1974-1975: Adjunct Lecturer at American University, Washington, DC.

(d) Professional associations: ACM/IEEE-CS, SUGI, NESUG;
PSU Computer Science and Engineering Curriculum/CQI Committee.

(2) I have reviewed United States Patent Application # 10/037,382 (Patent Application), further identified above, and the claims that are currently pending in the Patent Application and referred to in the Office Action received from the US Patent and Trademark Office dated October 6, 2005 (OA). In particular, I understand that claim 1 states that a portable 2-way secure purchasing aid logistics appliance comprises a secure memory coupled to a central processor to safeguard personal and financial information.

(3) I am not associated with the owner (Lockheed Corporation) or inventors (Joseph Claude Caci et al.) of the Patent Application nor do I know the inventors.

(4) I have reviewed the OA, and the cited reference in the OA, Petrovich et al., United States Patent Number 6,101,483, issued August 8, 2000 (Petrovich). Passages from the OA that are relevant to claim 1 are as follows:

(a) The OA states, in paragraph 6 on page 4, that the cited reference, Petrovich et al., United States Patent Number 6,101,483, issued August 8, 2000 (Petrovich) is used to reject Applicants' claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Petrovich in view of Treyz et al. United States Patent Number 6,587,835, issued on July 1, 2003;

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

(b) The OA states, in paragraph 7 on pages 4-5, that Petrovich discloses a portable 2-way secure purchasing aid logistics appliance (40), comprising a secure memory coupled to a central processor to safeguard personal and financial information (col. 5, lines 19-22 and 55-61);

(c) The OA states, in paragraph 45, page 17, that Petrovich's access control meets the limitation of Applicants' secure memory because Applicants' secure memory appears to be referring to encryption, but encryption is not claimed in claim 1;

(d) The OA states, in paragraph 52, on page 19, that, as used in the Office Action, the PIN number unlocks secure memory; and

(e) The OA states, in paragraph 55, on page 19, that the shopping list and personal information are stored on the portable device (of Petrovich) which requires a PIN to access the information in memory, and therefore, there is a layer of security provided which qualifies it as secure memory.

(5) I have reviewed the document referenced in the response to the Office Action mailed on October 12, 2004, www.kernelthread.com/publications/security/ac.html, and verify that the document states the general definition of access control, which Petrovich states in the OA's cited passages (Petrovich, col. 5, lines 19-22 and 55-61), that is:

(a) An initialization procedure can be carried out on the portable terminal (40) by entering an appropriate code for security and identification purposes; and

(b) A personal identification number (PIN) can be used to guard against theft of the portable terminal (40) or in conjunction with a credit or debit card.

In other words, the cited passages from Petrovich describe what is commonly known in the art as access control.

(6) Petrovich, contrary to the Examiner's position in the OA, does not disclose secure memory as it is known to those of ordinary skill in the art of Computer Science, and the system of Petrovich leaves memory vulnerable after an unauthorized access. To support my position, I declare the following:

(a) Secure memory as used in the Patent Application is a term of art meaning a resource whose content or reference to the content (e.g. address lines) is modified in order

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

to protect it from unauthorized intrusion, which Petrovich does not disclose. Secure memory products are available for purchase, and may be purchased without reference to access control methodology (see, for example, www.convergenceplus.com/mar05%20security%2001.html). The Patent Application has set forth two ways in which a secure memory resource could be implemented: (1) encryption of data and (2) memory location address realignment, and has stated that there are other ways in which a secure memory resource could be made unavailable to a user who has gained unauthorized access to the memory by bypassing access controls (see paragraph 51, last sentence, of the Patent Application).

(b) If a user gains access to secure memory – memory in which the binary signals in memory have been systematically changed -- inspection of the memory patterns does not lead to deciphering the contents of memory unless the user understands the methodology that led to the systematic change, for example, of data and/or address information, during the securing process.

(c) A simple access control mechanism as disclosed by Petrovich does not allow a user to review secure memory unless the user additionally employs the methodology used to secure the memory to start with; non-secure memory, as disclosed by Petrovich, on the other hand, is in its original state and can be accessed by unauthorized users.

(7) I further declare there is an essential difference between the security procedures of Petrovich and the secure memory as set forth in the claims of the Patent Application as follows:

(a) Petrovich states procedures that are generally referred to in the art as access control (e.g. Petrovich, col. 7, lines 26-27). The term, "access control" is commonly used by those of ordinary skill in the art to describe a method to determine if access should be granted to a resource. The description in Petrovich is limited to access control.

(b) The Patent Application refers to the deficiencies of simply employing an access control method as follows: "[F]inancial transactions require encryption to keep sensitive data secure. Communications encryption is accomplished today using the Public Key Infrastructure or PKI. This method is safe and secure as long as the key is safe and secure. If someone steals a laptop computer, the key is stored in the computer and it is

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

compromised. In the prior art, the public key is offloaded from the laptop computer to a smartcard. The smartcard must be inserted to make a secure connection. *However the memory of the laptop computer is still unprotected leaving stored data susceptible to theft* [Emphasis added] (Patent Application, paragraph 4), and "[T]he common practice is to lock the keyboard and display with a password. If a thief can steal a password then entry could be made on a desktop. Encrypted RAM could then protect sensitive information" (Patent Application, paragraph 48). In other words, the Patent Application clearly states that access control does not protect data that are stored in memory against unauthorized access, but an implementation of secure memory such as encrypted RAM would protect the data. Petrovich does not recognize such a distinction.

(c) FIG. 9 of the Patent Application illustrates access control and secure memory. In steps 1, 2, and 3, the user enters information in order to access and unlock secure memory. In step 4, if the access control information is invalid, data in secure memory are destroyed. Otherwise, secure memory is unlocked. If, for example, a user gains unauthorized access, the user still cannot access the data in secure memory because the secure memory requires unlocking before it can be accessed. In other words, the Patent Application and claims rely on conventional access control techniques as well as secure memory, as clearly seen from FIG. 9, whereas Petrovich simply relies on access control techniques as explained in paragraph (4) above.

(d) The Patent Application illustrates an example of secure memory in amended FIG. 8 (shown as Encrypted RAM 20A, having special read circuitry 23 and write circuitry 22). The Patent Application states that "[T]he secure memory of the present invention, illustrated in FIG. 8, is included in a memory map 70, the most basic element of any computing device" (Patent Application, amended paragraph 44), and "[E]ncrypted RAM 20A has the same general properties of RAM 10A in that memory can be read from and written to. . . By way of read circuitry 23 and write circuitry 22A encrypted RAM 20A functions as ordinary memory when set to secure mode. When encrypted RAM 20A is set disabled the data retrieved by way of read circuitry 23 is not logical and therefore useless. Write circuitry 22A does not function in a logical manner when disabled." (Patent Application, amended paragraph 46). In other words, the Patent Application discloses a secure memory which can be set to secure mode or disabled in which case data cannot be

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

read. On the contrary, Petrovich does not disclose features necessary to implement secure memory such as, for example, write circuitry that does not function logically when secure memory is set disabled. Thus, Petrovich does not disclose secure memory as claimed in the Patent Application, claim 1.

(e) The Patent Application states that "FIG. 11 is a flow chart of the address encrypted RAM of the secure memory of the present invention" (Specification, paragraph 18). The Patent Application further states that "FIG. 11 is an alternative embodiment of encrypted RAM. A portion of the RAM map 70, as shown in FIG. 8, is set aside for secure memory. A special address decoder 55 and an address tracker 56A generate the memory select lines using one of several possible mathematical formulae. . . . The contents of a memory location are not encrypted but its address is intentionally misaligned by a random number incorporated into the address decoder. . . . Using encrypted RAM, the central processor 11 cannot accurately track where data is physically stored. It depends on the address decoder 55 to correctly interpret the hexadecimal address." (Patent Application, amended paragraphs 50-52). In other words, secure memory can be implemented through address misalignment. Thus, securing memory is not limited to encrypting data. Clearly, simple access control requires no such address misalignment, and further, Petrovich discloses no such features.

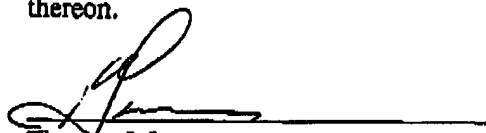
(8) In conclusion, I further declare that:

- (a) Secure memory as used in the Patent Application and claims is a term of art.
- (b) The Patent Application has set forth ways in which a secure memory resource could be implemented, and Petrovich, on the contrary, has set forth no such features.
- (c) If a user gains access to secure memory, i.e. if access control measures have failed, the user cannot automatically access the data in the secure memory.
- (d) A simple access control mechanism such as the PIN number provision in Petrovich does not protect memory when the access control mechanism is bypassed.

(9) All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true, these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or

Attorney Docket No. 12078-129
Appl. Serial No. 10/037,382

imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and such willful false statements may jeopardize the validity of the application or any patent issued thereon.



Thomas J. Leso
535 East Irvin Avenue
State College, PA 16801

FEBRUARY 1, 2006
Date